Exhibit A

Safety Feature	Operating System	Deficiency
Unknown AirTag Screen Alerts	iOS	• **Alert is not immediate**. Originally, the alert would not be triggered until 72 hours. Presently, the time has been shortened to between 4 and 8 hours, but this is still too dangerous a wait time. • **Can be disabled inadvertently**. iPhone owners who disable "Location Services" in their phone settings (which is often done for separate, privacy-related reasons) will also be unable to receive Unknown AirTag Alerts, but this consequence is not explained to users. • **Cannot be triggered independently**. A common problem—including for multiple Plaintiffs—is that Apple's alert cannot be triggered by the tracked individual. Instead, it pops up at random. Thus, the tracked individual often cannot rely on Apple's alerts if she wishes to seek further help. Or at least, she only may do so if the alert randomly pops up again, in the presence of the person from whom the tracked individual is seeking help (law enforcement; mechanic; friend; etc.). • **Reliability**. The iOS AirTag detection software has reported problems regarding (1) consistency and (2) accuracy.
Sound Alerts	iOS and Android	• **Alert is not immediate**. *See supra*. • **Cannot be triggered independently**. *See supra*. • **Volume is insufficient**. The AirTag alert volume is, at maximum, 60 decibels. This is not loud enough to ensure that an individual is alerted, particularly if the AirTag is muffled due to being placed on the outside of an individual's car, within a purse, wrapped in a noise-cancelling fabric, etc. • **Sound is not distinct.** The AirTag chime is indistinguishable from the myriad other sound alerts that people's phones, computers, smartwatches, and the like emit on a constant basis. Nothing about the AirTag chime alerts individuals to the significance of its purpose and context. Many individuals—including multiple Plaintiffs—where not aware of the significance of the AirTag sound alert upon hearing it.

		• **Duration**. The AirTag beep is not continuous and will stop before a targeted person can locate the AirTag. • **Can be disabled with ease**. As noted above, the AirTag remains functional even when the speaker has been disabled, which fact has been cognized by many would-be abusers, who have posted online tutorials on how to disable AirTag speakers for more effective stalking.
Disabling AirTags	iOS and Android	• **Physical possession of the AirTag is required**. If an individual wishes to disable an AirTag that is being used to stalk her, she must do so manually. This means that she needs to (1) find the AirTag, and (2) pop off the cover to remove the battery.[1] However, finding the AirTag is not always possible; or else it might require significant cost – for example, multiple Plaintiffs have been told by mechanics that their whole car would have to be stripped to look for the AirTag (a considerable cost). Further, physically dismantling the AirTag necessarily compromises evidence that would later needed in any law enforcement action.
AirTag Identifier Reset	iOS (and potentially Android)	• **Resetting identifiers also resets Apple's unknown tracker search logic.** Publicly available reporting,[2] indicates that an AirTag's identifier(s) automatically change at regular intervals, in order to be privacy protective of the owners. The problem, however, is that when those identifiers re-set, it appears to thwart Apple's "tracking alert logic."[3]
AirTag Firmware Updates	iOS (and potentially Android)	• **Relies on AirTag owners (i.e., stalkers) to implement.** Many of Apple's attempts to retroactively improve AirTag safety occur via

[1] https://support.apple.com/en-us/HT212227

[2] https://www.macworld.com/article/345863/how-to-find-block-disable-airtag-moving-with-you.html ("Another reason why you may not be able to find the AirTag is that it may have changed its identifier (which happens regularly). The Bluetooth ID produced by an AirTag, and by all Apple devices that participate in Find My crowdsourcing, changes on a regular basis to avoid becoming a reverse tracking item: if it were persistent, then someone could track your devices based on the "anonymous" Bluetooth ID. That means that your iPhone or iPad has to notice an AirTag moving with it over a relatively short period of time."

[3] *Id.*

		updates of AirTag firmware. For example, firmware update 2.0.24 enabled a feature wherein iPhone owners who are being tracked could use a precision finding feature to locate an unwanted AirTag.[4] But such firmware updates do not happen automatically, or "over the air." Instead, they require the AirTag owners to implement the updates. In the stalking context, this means that these safety updates must be implemented by the very people who the updates are meant to thwart.
Tracker Detect App	Android	• **Low Awareness**. The Tracker Detect App is not bundled into Android operating systems or suite of apps that come with non-Apple manufacturers. In order to use this safety measure, individuals would have to know about it, in the first place, and then seek it out and download it. • **Does not run in the background.** Unlike Apple's iOS-specific alerts, Tracker Detect is not "always on," meaning that the user must independently trigger the scan. Thus, the app is only as effective as the user's intuition. • **Triggering sound alerts.** The Tracker Detect user must wait 10 minutes before having a "detected" AirTag emit a sound.[5] This is particularly important, as Tracker Detect does not allow for precision finding (i.e., the app does not guide the user towards the AirTag's location). Thus, the only way for a user of Tracker Detect to locate the AirTag is through triggering the sound.

[4] https://support.apple.com/en-us/102183

[5] https://thebinaryhick.blog/2022/01/08/androids-airtags-oof/